AFRL-OSR-VA-TR-2013-0588

(MURI-08) A FRAMEWORK FOR MANAGING THE ASSURED INFORMATION SHARING LIFECYCLE

TIMOTHY FININ

UNIVERSITY OF MARYLAND BALTIMORE COUNTY

11/06/2013
Final Report

AIR FORCE RESEARCH LABORATORY
AF OFFICE OF SCIENTIFIC RESEARCH (AFOSR)/RSL
ARLINGTON, VIRGINIA 22203
AIR FORCE MATERIEL COMMAND

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 04-11-2013	**2. REPORT TYPE** FInal report	**3. DATES COVERED** *(From - To)* 01-05-2008 - 31-07-2013

4. TITLE AND SUBTITLE

A Framework for Managing the Assured Information Sharing Lifecycle

5a. CONTRACT NUMBER
FA9550-08-1-0265

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Tim Finin

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

University of Maryland, Baltimore County
Baltimore, MD 21250

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Dr. Robert L. Herklotz
Air Force Office of Scientific Research (AFOSR/RSL)
Suite 325, Room 3112
875 N. Randolph Street
Arlington, VA 22203-1768

10. SPONSOR/MONITOR'S ACRONYM(S)

AFOSR / RSL

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Public

13. SUPPLEMENTARY NOTES

14. ABSTRACT

AISL (Assured Information Sharing Lifecycle) is a MURI project that is developing new approaches to support assured information sharing. The team includes researchers from UMBC, Purdue University, and the Universities of Illinois, Michigan, Texas at Dallas, and Texas at San Antonio. Our current research efforts are organized around four areas: (1) creating novel assured information sharing models and frameworks and new policy languages and systems that support them, (2) developing algorithms and systems for information integration, analysis and mining that assure quality and protect privacy, (3) analyzing social aspects of information sharing including incorporating incentives for sharing and exploiting knowledge of underlying social networks and relations, and (4) implementing and evaluating experimental software architectures and systems to realize the assured information sharing life cycle. Our fourth year was productive with significant results achieved across all areas of the project.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Tim Finin
a. REPORT U	**b. ABSTRACT** U	**c. THIS PAGE** U	UU		**19b. TELEPHONE NUMBER** *(include area code)* 410-455-3522

A Framework for Managing the Assured Information Sharing Lifecycle

Final Report 5/2008-5/2012, AFOSR MURI FA9550-08-1-0265

Program Manager: Dr. Robert L. Herklotz, AFOSR

PI: Dr. Timothy W. Finin, University of Maryland, Baltimore County

Introduction

AISL (Assured Information Sharing Lifecycle) is a MURI project that is developing new approaches to support assured information sharing. The team includes researchers from UMBC, Purdue University, and the Universities of Illinois, Michigan, Texas at Dallas, and Texas at San Antonio. Our research efforts were organized around four areas: (1) creating novel assured information sharing models and frameworks and new policy languages and systems that support them, (2) developing algorithms and systems for information integration, analysis and mining that assure quality and protect privacy, (3) analyzing social aspects of information sharing including incorporating incentives for sharing and exploiting knowledge of underlying social networks and relations, and (4) implementing and evaluating experimental software architectures and systems to realize the assured information sharing life cycle. Our fourth year was productive with significant results achieved across all areas of the project. We briefly describe some of these results below and list selected recent publications.

Purdue University

Bertino and collaborators have developed the foundations for a new access control model that overcomes drawbacks of well-known existing access control models (namely RBAC and XACML). The language associated with the proposed model, called eXtensible Functional Language for Access Control (xfACL), is based on a functional notation. Dr. Clifton along with student Ahmet Erhan Nergiz have been working on techniques for processing partially encrypted databases, ensuring ability to share data that can be shared while protecting data that must be protected. Instead of separating disclosable and non-disclosable data (and thus potentially losing linkages between them), this technology will enable a single database that to the view of an appropriately authorized user shows the entire data, but to a lower authority user (including the server itself) shows only a limited view of the data. Clifton also worked with team member Murat Kantarcioglu at the University of Texas at Dallas on learning from data where adversaries are actively altering the data to "hide their tracks".

University of Illinois

The UIUC Team continued research on the theme of *integrating, mining and assessing the quality of shared information.* To this end, they have published over 200 papers in major conferences and journals and developed new models and algorithms for a number of key problems such as trust modeling and propagation, opinion integration and summarization, and latent topic structure mining. The following are a few highlights of their recent accomplishments.

Assessing trustworthiness of text data is very important for the information management component of their whole project, but it poses special challenges due to the difficulty in natural language understanding. To solve this problem, they extended a trust framework that they developed previously (i.e., TruthFinder) and they proposed a more general new unified trust propagation framework to compute trustworthiness scores for sources and textual claims in presence of quality measurements for evidence provided by humans. They instantiated the framework to model trustworthiness of news and predict if coverage on a given topic is trustworthy. Evaluation results show that the proposed new framework is effective for modeling trust of text data.

Integration and summarization of scattered opinions collected from multiple sources in an information sharing framework are critical to enable effective use of the shared information. They have developed a number of general techniques for integrating scattered opinions and summarizing them. First, they developed a general strategy for leveraging online ontology to organize scattered opinions into meaningful aspects. Second, they proposed a novel summarization algorithm for generating concise, abstractive summaries of redundant opinions Third, they proposed a novel opinion analysis problem called Latent Aspect Rating Analysis and developed two probabilistic models for solving this problem, which enable detailed analysis of opinions expressed in vast amount of online reviews by decomposing overall ratings into ratings on each specific aspect and inferring relative weights placed by reviewers on different aspects.

The Illinois team has developed a graph-based regularization framework, GNetMine, to model the link structure in heterogeneous information networks with arbitrary network schema and number of object/link types. Specifically, they explicitly differentiate the multi-typed link information by incorporating it into different relation graphs. Efficient computational schemes are introduced to solve the corresponding optimization problem. Experiments on the DBLP data set show that their algorithm significantly improves the classification accuracy over existing state-of-the-art methods (including both network/graph classification methods and their recently developed rank-based clustering methods). Furthermore they integrate ranking with heterogeneous information network classification, and developed a RankClass algorithm, which iterative refine both ranking and classification in information networks which derives higher quality classification model as well as good ranking for each type of nodes in heterogeneous information networks. The experiments show that the method derives even better quality classification models than GNetMine.

Heterogeneous information networks, i.e., the logic networks involving multi-typed, interconnected objects, are ubiquitous. It is necessary to provide functions for these networks to find similar objects, e.g., similar authors and papers in a bibliographic network. Unfortunately, there is a lack of similarity definition among multi-typed networks and effective algorithms for similarity search in such networks. They proposed an intuitive meta-path-based similarity definition: A user can specify a meta path sequence of relations to determine similarity scores among linked objects. Multiple meta-paths can then be combined to address complex queries. While this definition is flexible to represent different similarity queries, it requires expensive computations (e.g., matrix multiplications), which is not affordable in large-scale information networks. Thus they developed an efficient solution that partially materializes short meta path and then concatenates them online to compute results. The proposed method could improve search performance by 20%~300%. Moreover, to further explore the power of meta paths, they study the selection and use of meta paths to predict links and relationships in heterogeneous networks and show training can be performed to select the critical meta-path to enhance the predictability in heterogeneous networks, which are verified in experiments on the DBLP datasets.

Data cubes play an essential role in data analysis and decision support. In a data cube, data from a fact table is aggregated on subsets of the table's dimensions, forming a collection of smaller tables called cuboids. When the fact table includes sensitive data such as salary or diagnosis, publishing even a subset of its cuboids may compromise individuals' privacy. In this study, they address this problem using differential privacy (DP), which provides provable privacy guarantees for individuals by adding noise to query answers. They choose an initial subset of cuboids to compute directly from the fact table, injecting DP noise as usual; and then compute the remaining cuboids from the initial set. Given a fixed privacy guarantee, they show that it is NP-hard to choose the initial set of cuboids so that the maximal noise over all published cuboids is minimized, or so that the number of cuboids with noise below a given threshold is maximized. They provide an efficient procedure with running time polynomial in the number of cuboids to select the initial set of cuboids, such that the maximal noise in all published cuboids will be minimized. They also show how to enforce consistency in the published cuboids while simultaneously improving their utility (reducing error).

University of Maryland, Baltimore County

The UMBC team worked on three areas during the past progrsm: developing approaches and tools to enhance assured information sharing in social networking contexts, using policies and context to enforce privacy policies for information sharing in mobile devices such as smart phones, and applying policies and machine learning to detect malicious nodes in ad hoc networks.

They developed an implementation of he g-SIS group-centric access control model and demonstrate its usefulness to use cases in information sharing in social media. Contributions include the prototype implementation, extension to the model such as hierarchical groups and necessary and sufficient conditions, and the use of the semantic Web language OWL for representing the central g-SIS concepts and associated data. The framework uses a pragmatic approach of using semantic web technology to represent and reason about the hierarchy and procedural method to compute access decisions relying on the g-SIS semantics. They also developed a system that helps users maintain the information sharing groups typical of social networking systems like Facebook and Google+. They implemented a system that classifies a user's new connections into one or more existing groups based on the connection's attributes and relation and demonstrated the approach using data collected from real Facebook users. Another significant challenge is posed by hierarchical and overlapping groups. They showed that the system classifies new connections into these groups with high accuracy even with only 10-20% labeled data.

Recent years have seen a confluence of two major trends -- the increase of mobile devices such as smart phones as the primary access point to networked information and the rise of social media platforms that connect people. Their convergence supports the emergence of a new class of context-aware geo-social networking applications. While existing systems focus mostly on location, their work centers on models for representing and reasoning about a more inclusive and higher-level notion of context, including the user's location and surroundings, the presence of other people and devices, and the inferred activities in which they are engaged. A key element of the work is the use of collaborative information sharing where devices share and integrate knowledge about their context. This introduces the need for privacy and security mechanisms. They developed a framework to provide users with appropriate levels of privacy to protect the personal information their mobile devices are collecting including the inferences that can be drawn from the information. They used Semantic Web technologies to specify high-level, declarative policies that describe user information sharing preferences. They implemented and evaluated a prototype system that aggregates information from a variety of sensors on the phone, online sources, and sources internal to the campus intranet, and infers the dynamic user context. The policy framework can be effectively used to devise better privacy control mechanisms to control information flow between users in such dynamic mobile systems.

Mobile Ad-hoc Networks (MANETs) are extremely vulnerable to a variety of misbehaviors because of their basic features, including lack of communication infrastructure, short transmission range, and dynamic network topology. To detect and mitigate those misbehaviors, trust management schemes have been proposed that rely on pre-defined weights to determine how each apparent misbehavior contributes to an overall measure of trustworthiness. The extremely dynamic nature of MANETs makes it difficult, however, to determine a set of weights that are appropriate for all contexts. The UMBC group developed an automated trust management scheme for MANETs that uses machine learning to classify nodes as malicious. Our scheme is far more resilient to the context changes common in MANETs, such as those due to malicious nodes altering their misbehavior patterns over time or rapid changes in environmental factors, such as the motion speed and transmission range. The evaluation results on simulation studies showed it to be effective and to perform significantly better than other approaches.

University of Michigan

At the University of Michigan, Adamic and collaborators have conducted empirical and modeling studies of two aspects of assured information sharing. The first is determining whether ratings of information can themselves be relied upon. The second is discovering and measuring how multiple propagation steps can distort information as it is transmitted.

They examined the reliability of human-supplied ratings when individuals are asked to rate other individuals or the information they have provided. Last year they showed that ratings are inflated if they are given publicly, if they are identified, and if there is potential for reciprocity. This year, they followed up with a large scale data analysis of millions of user-to-user ratings, complemented by a survey of over 500 users of the website Couchsurfing.org, and 18 in-depth interviews. In order to understand the ratings, they revisit the notions of friendship and trust and uncover an asymmetry: close friendship includes trust, but high levels of trust can be achieved without close friendship. To users, providing faceted ratings presents challenges, including differentiating and quantifying inherently subjective feelings such as friendship and trust, concern over a friend's reaction to a rating, and knowledge of how ratings can affect others' reputations. One consequence of these issues is the near absence of negative feedback, even though a small portion of actual experiences and privately held ratings are negative. They show how users take this into account when formulating and interpreting ratings, and discuss designs that could encourage more balanced feedback.

Information dissemination is becoming increasingly more distributed, especially with increased use of social media. In social media content often makes multiple hops, and consequently has opportunity to change. In this paper they focus on content that should be changing the least, namely quoted text. They find changes to be frequent, with their likelihood depending on the authority of the copied source and the type of site that is copying. They uncover patterns in the rate of appearance of new variants, their length, and popularity, and develop a simple model that is able to capture them. These patterns are distinct from ones produced when all copies are made from the same source, suggesting that information is evolving as it is being processed collectively in online social media.

University of Texas, San Antonio

To share information and retain control (share-but-protect) is a classic cyber security problem for which effective solutions continue to be elusive. Where the patterns of sharing are well defined and slow to change, it is reasonable to apply the traditional access control models of lattice-based, role-based and attribute-based access control, along with discretionary authorization for further fine-grained control as required. This dissemination-centric approach offers considerable flexibility in terms of controlling a particular information object with respect to already defined attributes of users, subjects and objects. However, it has many of the same or similar problems that discretionary access control manifests relative to role-based access control. In particular specifying information sharing patterns beyond those supported by currently defined authorization attributes is cumbersome or infeasible. Therefore, UTSA researchers have developed and formalized a novel mode of information sharing called group-centric. Group-centric secure information sharing (g-SIS) is designed to be agile and accommodate ad hoc patterns of information sharing. A g-SIS theory has been developed for isolated groups, which are essentially sinks wherein information is brought into a group (akin to a secure meeting room) to be shared by group members. New information is also developed within the group. The UTSA team is currently extending the theory to connected groups wherein information in one group can be made accessible to members of another group by various subordination relations.

University of Texas, Dallas

Kantarcioglu, Thuraisingham, Khan and Bensoussan have worked on incentive compatible distributed data mining schemes, economic incentives privacy-preserving technology adoption, cloud computing based tools for assured information sharing and social network privacy issues. The group's incentive compatible distributed data mining results indicate that they can encourage truthful data sharing that does not require the ability to audit or verify the data under cooperative coalition formation scenarios. They prove that these mechanisms are incentive compatible under reasonable assumptions. In addition, they provide extensive experimental data that shows the viability of the mechanisms in practice. Our economic analysis of privacy-preserving technology (PPT) adoption indicates that in many cases significant government subsidies are needed to encourage PTT adoption. For cases where few individuals value privacy and are extremely profitable to a firm than there is a possibility for market based solutions. They developed new social graph anonymization scheme to protect against sensitive value inference attacks. We are collaborating with Dr. Steve Barker (he is funded by EOARD) to demonstrate assured information sharing using the secure cloud data and policy management system they have developed at UTD. This system was demonstrated at the September 2011 meeting in Washington DC.

Recent Publications

- Zhenhui Li, Jingjing Wang, and Jiawei Han, "Mining Periodicity for Sparse and Incomplete Event Data", Proc. 2012 ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, Aug. 2012
- Jingjing Wang and Bhaskar Prabhala, "Periodicity Based Next Place Prediction", Proc. Workshop on Mobile Data Challenge by Nokia, Newcastle, UK, June 2012.
- Zhijun Yin, Liangliang Cao, Jiawei Han, Chengxiang Zhai, and Thomas Huang, "LPTA: A Probabilistic Model for Latent Periodic Topic Analysis", Proc. 2011 IEEE Int. Conf. on Data Mining, Dec. 2011.
- Hongbo Deng, Jiawei Han, Michael R. Lyu and Irwin King, "Modeling and Exploiting Heterogeneous Bibliographic Networks for Expertise Ranking", Proc. 2012 ACM/IEEE Joint Conf. on Digital Libraries, Washington, D.C., June 2012. (Vannevar Bush Best Paper Award)
- Yizhou Sun, Brandon Norick, Jiawei Han, Xifeng Yan, Philip S. Yu, and Xiao Yu, "Integrating Meta-Path Selection with User Guided Object Clustering in Heterogeneous Information Networks", ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, Aug. 2012 (Best Student Paper Award)
- Ming Ji, Binbin Lin, Xiaofei He, Deng Cai, Jiawei Han, "Parallel Field Ranking", ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining, Beijing, China, Aug. 2012 (KDD'12 Best Paper award nominee, Best Poster Award, invited to the special issue of ACM Transactions on KDD)
- Yuannhua Lv, ChengXiang Zhai, Lower-bounding term frequency normalization. Proc. 2011 ACM int. conf. on Information and knowledge management, Nov. 2011 (Best Student Paper Award)
- Duo Zhang, ChengXiang Zhai, Jiawei Han, MiTexCube: MicroTextCluster Cube for Online Analysis of Text Cells. Proc. 2011 NASA Conf. on Intelligent Data Understanding, Oct, 2011.
- Liangliang Cao, Hyun Duk Kim, Min-Hsuan Tsai, Brian Cho, Zhen Li, Indrani Gupta, Chengxiang Zhai and Thomas Huang, Delta-SimRank Computing on MapReduce, Prof. 1st Int. Workshop on Big Data, Streams and Heterogeneous Source Mining: Algorithms, Systems, Programming Models and Applications, Aug. 2012 (Best Paper Award)
- The Role of Social Networks in Information Diffusion, Eytan Bakshy, Itamar Rosenn, Cameron Marlow, Lada A. Adamic, WWW'12.
- Recipe recommendation using ingredient networks. Chun-Yuen Teng, Yu-Ru Lin, Lada A. Adamic, WebSci 2011. Group Membership and Diffusion in Virtual Worlds,David A. Huffaker, Chun-Yuen Teng, Matthew P. Simmons, Liuling Gong, Lada A. Adamic, IEEE SocialCom 2011.
- Coevolution of network structure and content, Liuling Gong, Chun-Yuen Teng, Avishay Livne, Celso Brunneti, Lada Adamic, WebSci 2011.

- Memes Online: Extracted, Subtracted, Injected, and Recollected, Matthew P. Simmons, Lada A. Adamic, Eytan Adar, ICWSM 2011.
- Rating Friends Without Making Enemies, Lada A. Adamic, Debra Lauterbach, Chun-Yuen Teng, Mark S. Ackerman, ICWSM 2011.
- Jaewoo Lee and Chris Clifton, Differential Identifiability, The 19th ACM SIGKDD Conf. on Knowledge Discovery and Data Mining, Beijing, Aug. 2012.
- Elisa Bertino: Data Protection from Insider Threats, Morgan & Claypool Publishers, 2012.
- Ashish Kundu, Mikhail J. Atallah, Elisa Bertino: Leakage-free redactable signatures. CODASPY 2012: 307-316
- Ninghui Li, Haining Chen, Elisa Bertino: On practical specification and enforcement of obligations. CODASPY 2012: 71-82
- Alfredo Cuzzocrea, Elisa Bertino, Domenico Saccà: Towards a theory for privacy preserving distributed OLAP. EDBT/ICDT Workshops 2012: 221-226
- Hyo-Sang Lim, Gabriel Ghinita, Elisa Bertino, Murat Kantarcioglu: A Game-Theoretic Approach for High-Assurance of Data Trustworthiness in Sensor Networks. ICDE 2012: 1192-1203
- Russell Paulet, Md. Golam Kaosar, Xun Yi, Elisa Bertino: Privacy-Preserving and Content-Protecting Location Based Queries. ICDE 2012: 44-53
- Mohamed Nabeel, Elisa Bertino: Privacy preserving delegated access control in the storage as a service model. IRI 2012: 645-652
- Mohamed Nabeel, Ning Shang, Elisa Bertino: Efficient privacy preserving content based publish subscribe systems. SACMAT 2012: 133-144
- Basit Shafiq, Jaideep Vaidya, Arif Ghafoor, Elisa Bertino: A framework for verification and optimal reconfiguration of event-driven role based access control policies. SACMAT 2012: 197-208
- Rafae Bhatti, Ryan LaSalle, Rob Bird, Tim Grance, Elisa Bertino: Emerging trends around big data analytics and security: panel. SACMAT 2012: 67-68
- M. Nabeel, J. Zage, S. Kerr, E. Bertino, N. Athula Kulatunga, U. Sudheera Navaratne, M. Duren: Cryptographic Key Management for Smart Power Grids - Approaches and Issues CoRR abs/1206.3880: (2012)
- Weili Han, Ye Cao, Elisa Bertino, Jianming Yong: Using automated individual white-list to protect web digital identities. Expert Syst. Appl. 39(15): 11861-11869 (2012)
- Ashish Kundu, Elisa Bertino: On Hashing Graphs. IACR Cryptology ePrint Archive 2012: 352 (2012)
- Ashish Kundu, Mikhail J. Atallah, Elisa Bertino: Efficient Leakage-free Authentication of Trees, Graphs and Forests. IACR Cryptology ePrint Archive 2012: 36 (2012)
- Anna Cinzia Squicciarini, Elisa Bertino, Alberto Trombetta, Stefano Braghin: A Flexible Approach to Multisession Trust Negotiations. IEEE Trans. Dependable Sec. Comput. 9(1): 16-29 (2012)
- Michael S. Kirkpatrick, Gabriel Ghinita, Elisa Bertino: Resilient Authenticated Execution of Critical Applications in Untrusted Environments. IEEE Trans. Dependable Sec. Comput. 9(4): 597-609 (2012)
- Michael S. Kirkpatrick, Gabriel Ghinita, Elisa Bertino: Privacy-Preserving Enforcement of Spatially Aware RBAC. IEEE Trans. Dependable Sec. Comput. 9(5): 627-640 (2012)
- Ali Inan, Murat Kantarcioglu, Gabriel Ghinita, Elisa Bertino: A Hybrid Approach to Private Record Matching. IEEE Trans. Dependable Sec. Comput. 9(5): 684-698 (2012)
- Md. Enamul Kabir, Hua Wang, Elisa Bertino: A role-involved purpose-based access control model. Information Systems Frontiers 14(3): 809-822 (2012)
- James Joshi, Elisa Bertino, Calton Pu, Heri Ramampiaro: Mobile Networks and Applications Special Issue "Collaborative Computing: Networking, Applications and Worksharing". MONET 17(3): 325-326 (2012)
- Ilsun You, Gabriele Lenzini, Marek R. Ogiela, Elisa Bertino: Defending against insider threats and internal data leakage. Security and Communication Networks 5(8): 831-833 (2012)
- M. Kantarcioglu and W. Jiang, “Incentive compatible privacy-preserving data analysis”, IEEE TKDE, to appear, 2012.
- R. Nix, M. Kantarcioglu. “Incentive Compatible Privacy-Preserving Distributed Classification.” IEEE TDSC Special Issue on Learning, Games, and Security. 2012.

- R. Nix, M. Kantarcioglu, and K. Han. “Approximate Privacy-Preserving Data Mining on Vertically Partitioned Data.” DBSec 2012
- R. Nix, M. Kantarcioglu. “Game Theoretic Methods for Fast Query Verification on Outsourced Data.” Gamesec 2012.
- Chengcui Zhang, James Joshi, Elisa Bertino, Bhavani M. Thuraisingham: IEEE 13th International Conference on Information Reuse & Integration, IRI 2012, Las Vegas, NV, USA, August 8-10, 2012 IEEE 2012
- Abhijith Shastry, Murat Kantarcioglu, Yan Zhou, Bhavani M. Thuraisingham: Randomizing Smartphone Malware Profiles against Statistical Mining Techniques. DBSec 2012: 239-254
- Kerim Yasin Oktay, Vaibhav Khadilkar, Bijit Hore, Murat Kantarcioglu, Sharad Mehrotra, Bhavani M. Thuraisingham: Risk-Aware Workload Distribution in Hybrid Clouds. IEEE CLOUD 2012: 229-236
- Pranav Parikh, Murat Kantarcioglu, Vaibhav Khadilkar, Bhavani M. Thuraisingham, Latifur Khan: Secure information integration with a semantic web-based framework. IRI 2012: 659-663
- Jan Kallberg, Bhavani M. Thuraisingham: Towards cyber operations - The new role of academic cyber security research and education. ISI 2012: 132-134
- Pallabi Parveen, Bhavani M. Thuraisingham: Unsupervised incremental sequence learning for insider threat detection. ISI 2012: 141-143
- James R. (Bob) Johnson, Anita Miller, Latifur Khan, Bhavani M. Thuraisingham: Extracting semantic information structures from free text law enforcement data. ISI 2012: 177-179
- Satyen Abrol, Latifur Khan, Vaibhav Khadilkar, Bhavani M. Thuraisingham, Tyrone Cadenhead: Design and implementation of SNODSOC: Novel class detection for social network analysis. ISI 2012: 215-220
- Yan Zhou, Murat Kantarcioglu, Bhavani M. Thuraisingham, Bowei Xi: Adversarial support vector machine learning. KDD 2012: 1059-1067
- Bhavani M. Thuraisingham, Vaibhav Khadilkar, Jyothsna Rachapalli, Tyrone Cadenhead, Murat Kantarcioglu, Kevin W. Hamlen, Latifur Khan, Mohammad Farhan Husain: Cloud-Centric Assured Information Sharing. PAISI 2012: 1-26
- Tyrone Cadenhead, Vaibhav Khadilkar, Murat Kantarcioglu, Bhavani M. Thuraisingham: A cloud-based RDF policy engine for assured information sharing. SACMAT 2012: 113-116
- Elena Ferrari, Bhavani M. Thuraisingham: Guest Editors' Introduction: Special Section on Data and Applications Security and Privacy. IEEE Trans. Dependable Sec. Comput. 9(5): 625-626 (2012)
- Khalid Bijon, Tahmina Ahmed, Ravi Sandhu and Ram Krishnan, “A Lattice Interpretation of Group-Centric Collaboration with Expedient Insiders.” Proc. 8th IEEE Int. Conf. on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), Pittsburgh, Oct. 14-17, 2012.
- Khalid Bijon, Ravi Sandhu and Ram Krishnan, “A Group-Centric Model for Collaboration with Expedient Insiders in Multilevel Systems.” Proc. IEEE Int. Symposium on Security in Collaboration Technologies and Systems, Denver, CO, May 24th, 2012.
- R. Krishnan, J. Niu, R. Sandhu and W. Winsborough, “Group-Centric Secure Information-Sharing Models for Isolated Groups.” ACM Transactions on Information and System Security, v14, n3, Nov. 2011.
- Ravi Sandhu, K. Bijon, Xin Jin and Ram Krishnan, “RT-Based Administrative Models for Community Cyber Security Information Sharing.” 6th IEEE Int. Workshop on Trusted Collaboration, Oct. 2011.
- Wenjia Li, Anupam Joshi and Tim Finin, CAST: A Context-Aware Security and Trust Framework for Mobile Ad-hoc Networks Using Policies, Distributed and Parallel Databases, to appear, 2013.
- M. Lisa Mathews, Paul Halvorsen, Anupam Joshi and Tim Finin, A Collaborative Approach to Situational Awareness for CyberSecurity, 8th IEEE Int. Conf. on Collaborative Computing: Networking, Applications and Worksharing, Pittsburgh PA, 14-17 Oct 2012.
- Lushan Han, Tim Finin and Anupam Joshi, Schema-Free Structured Querying of DBpedia Data, Proc. 21st ACM Conf. on Information and Knowledge Management, Oct. 2012.
- Varish Mulwad, Tim Finin and Anupam Joshi, A Domain Independent Framework for Extracting Semantic Data from Tables, in Search Computing - Broadening Web Search, LNCS v7538, Springer, July 2012.

- Karuna P Joshi, Tim Finin, Yelena Yesha, Anupam Joshi, Navid Golpayegani and Nabil R. Adam, A Policy-based Approach to Smart Cloud Services, Service Research and Innovation Institute Global Conf., July 2012.
- Sumit More, Mary Mathews, Anupam Joshi, and Tim Finin, A Semantic Approach to Situational Awareness for Intrusion Detection, Proc. National Symposium on Moving Target Research, June 2012.
- Sumit More, Mary Mathews, Anupam Joshi and Tim Finin, A Knowledge-Based Approach To Intrusion Detection Modeling, Proc IEEE Workshop on Semantic Computing and Security, May 2012.
- D. Ghosh, Anupam Joshi, Tim Finin, and P. Jagtap, Privacy control in smart phones using semantically rich reasoning and context modeling, IEEE Workshop on Semantic Computing and Security, May 2012.
- A. Joshi, T. Finin, K. Joshi and M. Oberoi, A Policy Driven Semantic Approach to Data Usage Management, Workshop on Data Usage Management on the Web, Lyon, April 2012.
- Lushan Han, Tim Finin, Paul McNamee, Anupam Joshi, and Yelena Yesha, Improving Word Similarity by Augmenting PMI with Estimates of Word Polysemy, IEEE Transactions on Knowledge and Data Engineering, in press, 2013.
- Karuna Panda Joshi, Yelena Yesha, Tim Finin, and Anupam Joshi, Policy based Cloud Services on a VCL platform, Proc. 1st Int. IBM Cloud Academy Conf. (ICA CON 2012), April 1 2012.
- Wenjia Li, Palanivel Kodeswaran, Pramod Jagtap, Anupam Joshi and Tim Finin, Managing and Securing Critical Infrastructure - A Semantic Policy and Trust driven approach, in Securing Cyber-Physical Critical Infrastructures, Foundations and Challenges, pp. 551-572, Morgan Kauffman, Jan. 2012.
- Madan Oberoi, Pramod Jagtap, Anupam Joshi, Tim Finin and Lalana Kagal, Information Integration and Analysis: A Semantic Approach to Privacy, Proc. 3rd IEEE Int. Conf. on Information Privacy, Security, Risk and Trust, Oct. 2011.
- Wenjia Li, Anupam Joshi and Tim Finin, SAT: an SVM-based Automated Trust Management System for Mobile Ad-hoc Networks, Proc. 2011 Military Communications Conf., Nov.2011.
- Pramod Jagtap, Anupam Joshi, Tim Finin and Laura Zavala, Preserving Privacy in Context-Aware Systems, Proc. 5th IEEE Int. Conf. on Semantic Computing, Oct. 2011.